AO 106 (Rev. 04/010) Application for Search Warrant

UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of)
A BLACK ACER LAPTOP AND USB THUMB DRIVE)
CURRENTLY LOCATED AT 3301 WEST MEMORIAL) Case No: M-22-953-SM
ROAD, OKLAHOMA CITY, OK 73134)

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property *(identify the person or describe property to be searched and give its location)*:

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized)*:

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is (*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §2252A(a)(5)(B)	Possession of and accessing with intent to view child pornography

The application is based on these facts:

See attached Affidavit of Special Agent Charles Thumann, Federal Bureau of Investigation, which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Applicant's signature

Charles Thumann
Special Agent
Federal Bureau of Investigation

Sworn to before me and signed in my presence.

Date: 12/28/22

Judge's signature

City and State: Oklahoma City, Oklahoma

Suzanne Mitchell, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Charles W. Thumann, a Special Agent (SA) with Federal Bureau of Investigation, being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") since July 2004 and am currently assigned to the Oklahoma City Division, Norman Resident Agency. While employed by the FBI, I have received specific training and experience in numerous methods of investigation, including but not limited to, electronic and visual surveillance, general questioning of witnesses, the use of search warrants, the use of confidential sources/informants, the use of pen registers, and the use of undercover agent. Based on my training and experience related to the investigation of child pornography, and based upon interviews I have conducted with other officers, defendants, informants, and other witnesses and participants in child exploitation, I am familiar with the ways that child pornography in manufactured and distributed. My familiarity includes the various mean and method by which producers of child pornography manufacture and distribute pornography, their use of cellular telephones and computers. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the black ACER laptop and a USB thumb drive (referenced herein as the "SUBJECT DEVICES") which belong to Daniel Boice for

contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(5)(B) (possession and accessing of material containing child pornography). These devices are currently in the custody of the FBI at 3301 W. Memorial Road, Oklahoma City, OK 73134.

3. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of foregoing statute are presently located within the SUBJECT DEVICES.

DEFINITIONS

4. The following definitions apply to this Affidavit and Attachment B:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

b. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is

indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. "Cloud storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units; internal and peripheral storage devices such as fixed disks; external hard drives; "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer; and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. "Hyperlink," as used herein, refers to an item on a web page or in a mobile application which, when selected, transfers the user directly to another location in a hypertext document or to some other web page or (part of) a mobile application.

h. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

i. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be

directed properly from its source to its destination. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

j. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

k. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

l. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

m. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

n. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks; RAM; "thumb," "jump," or "flash" drives; CD/DVDs; and other magnetic or optical media.

o. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or

copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

p. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

5. The FBI is currently investigating child pornography trafficking by targets who created online accounts with a foreign based cloud-storage provider (referenced herein as "Cloud A"), and which accounts contained images and/or videos depicting child pornography. Specifically, the targeted users accessed and imported one or more files into their Cloud A account from one or more hyperlinks containing videos of the sexual exploitation of infants, toddlers and prepubescent children, to include those known to investigators as the series, "Daisy's Destruction," which depicts the sadistic sexual exploitation, torture, and abuse of a toddler. Cloud A is available to the general public for legitimate, non-criminal purposes, but investigation has revealed that some users engage in child pornography trafficking on this cloud-storage provider by means of sharing links to Cloud A folders containing child pornography. The current investigation targets individuals associated with such Cloud A accounts. As described herein, there is probable cause to believe that an individual or individuals associated with a Cloud A account containing child pornography will be found within the SUBJECT DEVICES.

OVERVIEW OF Cloud A

6. Cloud A is a cloud-based digital storage and file-hosting website and application based outside the United States.[1] An individual can access Cloud A through a web browser or through an application installed on a compatible mobile device. Users can upload electronic files and data to Cloud A for the purpose of storing and/or backing up their data, including image and video files. A Cloud A user can organize data into file folders within the user's account.

7. To create and subsequently log into a Cloud A account, a user must provide an e-mail address, which must be verified by Cloud A, and a unique password. The user's e-mail address functions as the user's Cloud A username. A Cloud A user account can access some digital storage free of charge or pay for additional storage.

8. From a browser, a Cloud A user can upload files to a Cloud A account by selecting the file or folder upload button. This button opens a dialog box in which the user can select the file or folder to upload. A user can also drag and drop a file or folder from their local device. From the Cloud A application installed on a mobile device, a user can upload files by clicking the circle icon with a plus symbol. This allows the user to navigate to files on their mobile phone or take a photo with the mobile phone's camera and directly upload the file or folder into the Cloud A account. Once files or folders are uploaded to a user's Cloud A account, the user can organize his/her stored data. A user's files are encrypted while stored on Cloud A and only the user can decrypt the files.

[1] The actual name of Cloud A is known to law enforcement but anonymized here to protect operational security.

9. A Cloud A account user can share files or folders in a Cloud A account by creating and sharing a hyperlink, expressed as a uniform resource locator ("URL"), to the specific files or folders of files in the Cloud A user's account.[2] Cloud A hyperlinks can be shared and the content at the links can be accessed by anyone who has access to the Internet (i.e., the recipient need not have a Cloud A account).[3]

10. In order to share a file or the contents of a Cloud A folder with another individual via hyperlink, a Cloud A account user (i.e., someone who has logged into a Cloud A account with the pertinent username and password) first selects file(s) or folder(s) to share. Next, the Cloud A account user may select "get link," which function can be used to create the folder handle – a list of characters which designate the location name for the file(s) or folder(s). A Cloud A user can choose to share the handle and decryption key as one combined URL or separately. For a shared file or folder to be opened, viewed, imported into a Cloud A user's account or downloaded to a digital device by means of a hyperlink, the recipient must have the associated decryption key. Without the decryption key, a file or contents within a folder would be inaccessible to anyone other than the account holder. The recipient of a Cloud A hyperlink need not have a Cloud A account to open, view or download the files or folders. To import files or folders into a Cloud A account, however, the user must have an active Cloud A account.

---

[2] Aside from creating and sharing hyperlinks, a Cloud A user could also give access to his Cloud A account by other means, such as by giving the account password to another individual to allow that individual to log into the user's Cloud A account with full access. A Cloud A user may also share files or folders privately with another user by invitation to specified e-mail addresses.

[3] Hyperlinks to files or folders of files on Cloud A are sometimes referred to as public hyperlinks and/or links.

11. Cloud A account users can give other Cloud A account users one of three access levels to shared folders: "Read Only," which allows downloading only; "Read/Write," which allows files and folders to be downloaded or added, but does not allow for modification or deletion of existing files and folders; or "Full Access," which allows downloading, addition, modification, and deletion of files and folders.

12. Cloud A also has a chat feature through which Cloud A users can send messages, files, and hyperlinks to other users. To view and participate in a chatroom on Cloud A, a user must have the associated link and decryption key for that chatroom, which can be provided via hyperlink. Anyone with the decryption key can view the chat. However, only Cloud A account users can post messages or links into the chat.

13. When individuals access Cloud A hyperlinks, they are presented with the files or folders included within the hyperlink. The default view is for the files to be shown as thumbnails or small representations of the content. For video files, the first frame of the content of the file will be shown. An individual can choose to represent the content of a hyperlink in a list format in which the file or folder content is displayed as a small icon with the file name, size, type, and date.

14. Once a Cloud A hyperlink is accessed, the user can choose to do any of the following actions:

a. View the file in the built in Cloud A file viewer;

b. Download the selected file or folder to the user's device (computer or mobile phone);

c. Import all content or selected files or folders into the user's Cloud A account; or

d. Create a new hyperlink for a selected file or folder.

15. Accessing a Cloud A hyperlink does not automatically result in the file or folders being added or imported into a user's Cloud A account. Rather, a user must purposefully decide to do so. For a user to import a file or folder from a Cloud A hyperlink, the user can right click the file or folder and select "import," or click the file menu button, which appears as three grey dots in a small white box, and import the file or folder. A Cloud A user can choose to import some or all the files or folders contained within a Cloud A hyperlink. When content has been imported into a Cloud A user's account in this manner, the hyperlink structure does not change. As a result, Cloud A can identify accounts in possession of files or folders contained in a Cloud A hyperlink.[4]

TARGET HYPERLINK 1

16. A foreign law enforcement agency ("FLA") in the same country in which Cloud A is located has reported to the FBI that on September 9, 2019, the FLA was notified of a public Cloud A hyperlink, TARGET HYPERLINK 1, containing photos and videos depicting the sexual exploitation of children.[5] The hyperlink contained a folder entitled "all" with five video files (one of which was inoperable) and eight sub-folders entitled: "125;" "baby;" "Girls;" "good quality;" "Keep;" "Pics;" "whiteking HD 1;" and "whiteking HD 2." The FLA reviewed the contents of the

[4] Cloud A can identify accounts in possession of files or folders contained in a Cloud A hyperlink even if the account user has since deleted the content. This investigation, however, only targeted Cloud A account users who still had the content contained within their Cloud A user account.

[5] The FLA is a national law enforcement agency of a country with an established rule of law. There is a long history of U.S. law enforcement sharing criminal investigative information with the FLA and the FLA sharing criminal investigative information with U.S. law enforcement, across multiple disciplines, including crimes against children. The FLA advised it was originally notified of Target Hyperlink 1 by another foreign law enforcement agency.

folder and sub-folders. The sub-folder "baby" contained 54 videos and 1 image. Many of the files in this sub-folder depicted the sexual exploitation of infants and toddlers, to include 4 videos from the series known to investigators as, "Daisy's Destruction," which depicts the sadistic sexual exploitation, torture, and abuse of a toddler. The sub-folder "125" contained 105 videos, mostly depicting the sexual exploitation of prepubescent minors.

TARGET HYPERLINK 2

17. The FLA has also reported to the FBI that on October 14, 2019, the FLA was notified of a second public Cloud A hyperlink, TARGET HYPERLINK 2, containing photos and videos of the sexual exploitation of children.[6] The FLA reviewed the contents of the folder and sub-folders. The folder structure and content were identical to that contained in TARGET HYPERLINK 1, minus the 5 videos contained in the "all" folder. Because this investigation focuses on the sub-folders "baby" and "125" both of which were identical in TARGET HYPERLINK 1 and TARGET HYPERLINK 2, they will hereinafter be referred to collectively as the TARGET HYPERLINKS. The FLA reported the TARGET HYPERLINKS to Cloud A, requested the hyperlinks be disabled and all content removed, and requested information from Cloud A about the sub-folders "baby" and "125."

INFORMATION ABOUT SUB-FOLDERS "BABY" and "125"

18. According to information the FLA provided to the FBI, the TARGET HYPERLINKS were public hyperlinks, meaning the decryption key was embedded within the

[6] The FLA advised it was originally notified of Target Hyperlink 2 by a foreign-based public reporting hotline for child exploitation material.

hyperlinks, and therefore any person with the hyperlinks (whether they had a Cloud A account or not) could view the content, download the content to a digital device, or import the content to a Cloud A account if they were a Cloud A account user. Cloud A accounts that accessed the TARGET HYPERLINKS had the ability to import some or all the content into their Cloud A accounts. Cloud A was able to identify all Cloud A accounts that imported all or a portion of the files from sub-folders "baby" and "125" contained in the TARGET HYPERLINKS in this manner.

19. Cloud A identified all Cloud A accounts that imported some or all files in the folders "baby" and "125." Cloud A then provided the following information regarding those accounts to the FLA: the Cloud A account name (the e-mail address used to create the account); the Cloud A account creation date and time; IP addresses (including the account creation IP, most commonly used IP, and last login IP); and a breakdown of the images and or videos from sub-folders "baby" and "125" that the Cloud A account had at the time the account was suspended by Cloud A.

TARGET IDENTIFICATION

20. In December 2019, the FLA provided evidence to the FBI of the Cloud A accounts resolving to the United States based on IP addresses that accessed and imported one or more of the files from the sub-folders "baby" and "125" from the TARGET HYPERLINKS. This investigation involves target Cloud A accounts that specifically imported at least one of the "Daisy's Destruction" files from the sub-folders "baby" and "125" from the TARGET HYPERLINKS.

21. As such, the Cloud A account name Upsilonalpha176@gmail.com (referenced herein as the "TARGET ACCOUNT"), with an account creation date of July 30, 2019, and IP

address 99.145.99.33, imported approximately 44 video files from the sub-folder "baby," including all four of the "Daisy Destruction" files on August 10, 2019, at 7:07:53 PM, and approximately 100 video files from the sub-folder "125" on August 10, 2019, at 7:07:53 PM, from the TARGET HYPERLINKS. These files were in the TARGET ACCOUNT as of approximately October 23, 2019, the date the TARGET ACCOUNT was closed by Cloud A. Your affiant has reviewed the files imported by the TARGET ACCOUNT from the TARGET HYPERLINKS. An example of the files imported into the TARGET ACCOUNT are described below:

a. File "01 primera parte.avi" (video contained in the Daisy's Destruction series) depicts a half-masked adult female playing with a prepubescent female toddler, both of Asian ethnicity. While on a mattress, the adult female removes her clothing along with the clothing of the female toddler and takes the female toddler's hand and rubs it on the adult female's breasts. The adult female grabs the prepubescent female toddler's head and places the female toddler's mouth on the adult female's breast. The adult female places the female toddler's hand and then mouth, on the adult female's vagina. A Caucasian adult male is seen video recording the conduct between the adult female and female toddler. The adult female places the female toddler on her back and slaps the female toddler's vagina. The adult female digitally penetrates the female toddler's vagina then places the finger used to penetrate the female toddler's vagina in the child's mouth. The adult female holds the female toddler's legs over her head as the adult female slaps the female toddler's buttocks and vagina multiple times. The adult female pinches and pulls the female toddler's nipples multiple times. The adult female puts the female toddler's hand in the adult female's vagina and then into the female toddler's mouth as the adult female slaps

the female toddler's head multiple times with the adult female's foot and hand. The adult female pushes the female toddler onto her back and spreads her vagina apart. The adult female then stands the female toddler up and hugs her while the adult female slaps the female toddler's buttocks. The adult female waves to the camera and directs the female toddler to wave "bye bye" to the camera. The adult female is seen slapping the female toddler's face as the video ends. The female toddler is seen and heard crying throughout the video. The video is 9 minutes and 10 seconds in duration.

b. File "daysy1.mp4" (video contained in the Daisy's Destruction series) depicts a half-masked naked adult female removing the diaper of a female toddler, both of Asian ethnicity. While on a mattress, the female toddler is lying on her back and the adult female takes what appears to be an ice cube and rubs it over the female toddler's chest, focusing on the child's nipples, and then around the child's vagina. The adult female attempts to insert the ice cube into the female toddler's vagina. An adult male voice can be heard in the background of the video and a Caucasian adult's hand is seen. The adult female ties the female toddler's ankles to a hanging device then suspends the female toddler upside down with the device. The adult female duct tapes the female toddler's hands to the bed and places a piece of duct tape across the female toddler's mouth. The adult female places what appears to be a plastic clip on both female toddler's nipples and then slaps the female toddler's vagina multiple times. The adult female places a plastic clip on the female toddler's vagina and places her tongue near the female toddler's vagina. The adult female takes an ice cube and rubs it on the prepubescent female toddler's chest then slaps and flicks the female toddler's vagina multiple times until it is visibly red. The adult female

removes the duct tape from the female toddler's hands and lifts the body of the female toddler upright, placing the female toddler's hands on the bar the female toddler's ankles are tied to, as the adult female slaps the female toddler's vagina and buttocks multiple times. The adult female retrieves a lighter and candle, placing both close to the female toddler's face while the adult female lights the candle. The adult female places the lit candle close to the female toddler's vagina. The prepubescent female toddler is seen and heard crying throughout the video. The video is 5 minutes and 43 seconds in duration.

c. File "daysy2.mp4" (video contained in the Daisy's Destruction series) depicts a half-masked adult female wearing a bikini standing over a naked female toddler tied to a hanging device by her ankles and lying on a mattress. Both appear to be of Asian ethnicity. The background of the video appears to be computer-generated imagery (CGI) of a dungeon. The adult female places her foot on the vaginal region of the female toddler and then suspends the female toddler upside down by her ankles from the device the child is tied to. The adult female removes her bikini top and places the mouth of the female toddler on the adult female's breasts. The adult female slaps the face of the female toddler with the bikini top. The adult female removes her bikini bottom and holds the hands of the female toddler behind her back while the adult female forces the face of the female toddler on the vagina of the adult female. The adult female duct tapes the wrists of the female toddler together behind her back and places the bikini bottoms in the mouth of the female toddler then places duct tape over her mouth. The adult female pinches and slaps the nipples, arms, and hands of the female toddler multiple times. The adult female punches and slaps the female toddler's head and slaps the female toddler's vagina. The adult female

rubs lubricant and a dildo on the female toddler's vagina. The hands of the female toddler are re-taped multiple times. The adult female punches the back of the female toddler's head multiple times throughout the process. The adult female inserts the dildo into the female toddler's vagina, twisting multiple times and inserting deeper, leaving the dildo inserted as the adult female retrieves a black band used to slap the body and face of the female toddler. The adult female uses her hand to slap the vagina of the female toddler before the dildo is removed from the female toddler's vagina. The adult female retrieves a candle and lighter. The adult female lights the candle and places it close to the face of the prepubescent female toddler and then over the vagina and nipple region of the female toddler. The adult female blows out the candle and retrieves the band, using it to slap the face and body of the female toddler. The adult female removes the tape from the female toddler's mouth and places the female toddler's mouth on the adult female's vagina. The prepubescent female toddler is seen and heard crying throughout the video. The video is 9 minutes and 40 seconds in duration.

d. File "daysy4.mp4" (video contained in the Daisy's Destruction series) depicts a half-masked naked adult female speaking in a foreign language to a female toddler, both of Asian ethnicity. While on a mattress, the adult female removes the diaper of the female toddler. The adult female licks the vagina of the female toddler then kisses the female toddler as the adult female digitally penetrates the child's vagina. The adult female carries the female toddler away from the mattress and camera. The adult female is then seen standing over a toilet as the female toddler is held upside down by an unknown person over the toilet. The adult female urinates on the female toddler's face. The adult

female then pours water over the female toddler's face and on the adult female's vagina. The female toddler is seen and heard crying throughout the video. The video is 2 minutes and 42 seconds in duration.

e. File "video_2018-11-19_03-04-49" depicts a fully naked prepubescent female sitting in a bathtub partially filled with water. The prepubescent female touches and rubs her vagina with her hand before using a purple dildo to rub her vagina. The prepubescent female continues to rub her vagina and chest. The prepubescent female repeatedly penetrated her vagina with the purple dildo while she remained in the partially filled bathtub. The prepubescent female then repeatedly placed the purple dildo inside her mouth. The prepubescent female continued to rub and penetrate her vagina with the purple dildo in various positions – standing, bending over, and sitting on the side of the bathtub. The prepubescent female then appears to use a cell phone before proceeding to get out of the bathtub and get fully dressed. The video is 13 minutes and 39 seconds in duration.

22. A query of the American Registry for Internet Numbers ("ARIN") online database revealed that IP address 99.145.99.33 was registered to AT&T. On January 8, 2019, a subpoena/administrative summons was issued to AT&T regarding the IP address 99.145.99.33 on July 30, 2019, at 08:18 UTC, described in Paragraph 21. The results identified the following account holder and address:

Established Date: 02/01/2019

Status: Active

Account Name: Daniel BOICE

Account Address: 1701 San Pablo Road S, Apt 211, Jacksonville, FL

Telephone: 251-214-1308

23. On March 26, 2020, an administrative subpoena was served on Google regarding email address Upsilonalpha176@gmail.com:

Google Account ID: 516234615554

Name: Dan BOICE

e-Mail: upsilonalpha176@gmail.com

Created on: 2012-02-09 05:25:58 UTC

Terms of Service IP: 69.85.195.254

Last Logins: 2020-03-05 03:17:16 UTC, 2020-01-18 23:22:33 UTC, 2019-07-30 08:10:57 UTC.

Email Address: dfboice@gmail.com

24. In April 2021, the aforementioned information was initially provided to the FBI Jacksonville Division. Public database checks identified BOICE's address as 1701 San Pablo Rd S, Apt 211, Jacksonville, FL. Public database checks identified BOICE's spouse, Kate Busselle, also resided at this address. A search of the Florida Department of Motor Vehicles identified 1701 San Pablo Rd S, Apt 211, Jacksonville, Florida, as Busselle's home address. Vehicle title and registration for a 2007 tan color Lincoln Utility identify the license plate type as "Navy" and the owner is Daniel Francis BOICE who resided at 1702 San Pablo Rd S, Apt 211, Jacksonville, Florida.

25. FBI Jacksonville received the information from FBI CEOU that BOICE was a U.S. Navy Reservist, E-5. NCIS was contacted and provided BOICE's military service records, which

included his college transcript. BOICE attended college at Spring Hill College in Mobile, Alabama.

26. In September 2021, FBI Jacksonville discovered BOICE and Busselle were no longer located in the Jacksonville, Florida area. FBI Jacksonville later learned BOICE and Busselle relocated to Norman, Oklahoma.

27. In November 2022, the original lead from FBI CEOU was forwarded from FBI Jacksonville to the FBI Oklahoma City Division, Norman Resident Agency.

28. On November 22, 2022, University of Oklahoma (OU) confirmed Busselle was hired as an Assistant Professor on August 16, 2021. OU provided Busselle's address as 3700 W. Tecumseh Rd, Apt 5304, Norman, Oklahoma.

29. On November 25, 2022, a public records search of the website of Upsilon-Alpha Chapter of Tau Kappa Epsilon at Spring Hill College listed Daniel F. BOICE in its member directory. BOICE was listed as member number 176 in the directory. Dan BOICE was identified as the name from the Google subpoena for email address Upsilonalpha176@gmail.com.

30. On November 25, 2022, a representative of the U.S. Postal Service confirmed that BOICE and Busselle currently receive mail at 3700 W. Tecumseh Rd, Apt 5304, Norman, Oklahoma.

31. On November 25, 2022, physical surveillance was conducted at 3700 W. Tecumseh Road, Norman, Oklahoma. This location is a large, three-story apartment complex. Two vehicles associated with Busselle and BOICE were observed in the parking lot near apartment 5304 where the vehicles were parked next to each other. A white Ford Escape, bearing Oklahoma license plate KSA834, is registered to Busselle. The parking spot immediately next to the Ford Escape was a

tan Lincoln Navigator, bearing military (U.S. Navy) Oklahoma license plate 0600NV1. The Lincoln Navigator is registered to BOICE.

32. A search of a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, and other information was conducted for BOICE. These public records indicated that BOICE's current address is 3700 W. Tecumseh Rd, Apt 5304, Norman, Oklahoma.

33. On December 13, 2022, FBI agents executed a federal search warrant issued by U.S. Magistrate Judge Shon T. Erwin at 3700 W. Tecumseh Rd, Apt 5304, Norman, Oklahoma and seized electronic devices within the apartment. During the search of the premises, agents conducted a voluntary interview of BOICE. BOICE confirmed the following: he was a member of Upsilon-Alpha Chapter of Tau Kappa Epsilon at Spring Hill College in Alabama, his cell phone number is 251-214-1308, and his email address is dfboice@gmail.com. BOICE later admitted the username and email address upsilonalpha176 was a holdover from his fraternity days. BOICE had a Cloud A account from 2015 through October 2019. BOICE was aware why his Cloud A account was suspended in October 2019 – his account contained child pornography. BOICE admitted he viewed the video described in paragraph 21(e.). BOICE further admitted to viewing child pornography on the Dark Web with the use of his laptop (one of the SUBJECT DEVICES). BOICE has viewed child pornography as recently as six months ago. BOICE provided his passcode for his cell phone and laptop to law enforcement. BOICE had two laptops, one in the apartment and another in his vehicle. BOICE provided agents consent to search his vehicle for his backpack which contained his black ACER laptop and USB thumb drive (SUBJECT DEVICES). BOICE confirmed his vehicle was a 2007 Lincoln Navigator with Oklahoma tag 0600NV1 (U.S.

Navy plate) and signed an FD-26 Consent to Search form. Agents proceeded to search BOICE's vehicle and seized the SUBJECT DEVICES from within the vehicle.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

34. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps

consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data. In sum, modern computers could very easily indefinitely contain evidence in 2022 of BOICE's 2019 (and later) child pornography activities described in this affidavit. These computers, including smart phones, can store huge amounts of information indefinitely. Digital child pornography files can be transferred back and forth between devices (e.g., synching a cell phone to a laptop computer, moving computer files to an external hard drive, etc.). Such files can also be stored simultaneously on multiple computers and other digital storage devices. Moreover, evidence of accessing Cloud A via

the internet (through a computer's browser history), downloading a Cloud A app, and other evidence of the crimes described in this affidavit could be indefinitely stored in modern computers. Computer forensic analysts very frequently find several-years-old evidence on computers during their analysis because computers have such enormous storage capacity that there is little or no reason for the user to delete such evidence to make room.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ENGAGE IN SEXUAL EXPLOITATION OF CHILDREN, SUCH AS THROUGH THE POSSESSION OF AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY—I.E., CHILD PORNOGRAPHY "COLLECTORS"

35. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to child pornography collectors:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or in other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain their pictures, films, video tapes, photographs, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, and child erotica, etc. for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment. These collections may exist on the individual's current as well as older cell phones, computers and tablets. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography and accessing cloud storage and evidence of use of cloud storage apps, often can be located on these individuals' computers and digital devices through the use of forensic tools.

Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[7]

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including email addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

36. Based on my training and experience, I know that people who use their computer/laptop to view/access/possess child pornography do so in private to avoid detection. I believe there is probable cause that the SUBJECT DEVICES found within BOICE's vehicle will contain evidence of the aforementioned criminal violations, as set for in detail in Attachment B.

[7] *See* United States v. Wagner, 951 F.3d 1232, 1246 (10th Cir. 2020) (Courts are less receptive to staleness challenges when the warrant concerns child pornography because persons interested in those materials are likely to hoard them in the privacy of their homes for significant periods of time); *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

37. Because the SUBJECT DEVICES are already in the custody of law enforcement, I request permission to execute the search at any time in the day or night.

CONCLUSION

38. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits, and instrumentalities of these offenses are located on the SUBJECT DEVICES. I respectfully request this Court issue a search warrant for the SUBJECT DEVICES, described in Attachment A, authorizing the seizure of the items in Attachment B to this affidavit.

Charles W. Thumann
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 28th day of December, 2022.

SUZANNE MITCHELL
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF THE SUBJECT DEVICES TO BE SEARCHED

- Black Acer Laptop with serial number NXHN1AA004020149677600; and
- USB thumb drive

which were seized from 2007 Lincoln Navigator with Oklahoma tag 0600NV1 (U.S. Navy) on December 13, 2022.

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. § 2252A(a)(5)(B):

1. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a) evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b) evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c) evidence of the lack of such malicious software;

d) evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e) evidence indicating the computer user's knowledge and/or intent as it relates to the

crime(s) under investigation;

f) evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g) evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h) evidence of the times the COMPUTER was used;

i) passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j) documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k) records of or information about Internet Protocol addresses used by the COMPUTER;

l) records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m) contextual information necessary to understand the evidence described in this attachment.

2. Routers, modems, and network equipment used to connect computers to the Internet.

3. Child pornography, as defined in 18 U.S.C. § 2256(8), and child erotica.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media

that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, USB drives, thumb drives, micro SD cards, macro SD cards, CD/DVDs, gaming systems, SIM cards, cellular phones capable of storage, memory cards, memory chips, and other magnetic or optical media.